

Cybercrime:

- How are cybercrime actors classified? Offer some examples
- Which are some direct ways to monetize cybercrime? Which are some indirect ways?
- What is ransomware, how does it work? Why did they rise to prominence lately?
- What is a botnet?
- What are some malware installation techniques?
- Which are the main components of the cybercrime ecosystem?
- What is a money mule?

Crypto and cybercrime:

- Why are cryptocurrencies so important in the cybercrime ecosystem?
- What is mining?
- Analyse pros and cons of bitcoins anonymity, and indicate additional measures used to strengthen it / What are mixers, shapeshifters? Why are they used?

Digital forensics intro:

- What does the Daubert standard establish?
- What can be considered as "scientific" in the context of digital forensics?

Source acquisition:

- What is the greatest forensic problem of digital evidence?
- Why are hashes/digital signatures used? Does a lack of hash collection during the acquisition procedure invalidate evidence?
- What is a write blocker and why is it useful?
- Describe the basic acquisition procedure, assuming a powered off system. What changes in case the target is on / disconnecting drives is complex?

Identification:

- How do HDDs filesystems work? Why is it possible to recover deleted data from them?
- What is carving?
- What are the main types of anti-forensic techniques? On which part of the forensic process do they interfere?
- Explain how one specific anti-forensic technique works.
- What are FTLs, why are they used and how do they interfere with SSD identification?
- What are the main challenges of cloud forensics?
- What are the main challenges of mobile forensics?

Evaluation and presentation:

- What should a technical expert be looking for when reviewing process documents?
- What are some common acquisition/analysis/presentation errors to look out for in reviewing process documents?
- Which high-level structure should a technical report follow? Explain each section
- What characteristics are important to write an effective report? What should be avoided, on the other hand?

- In a court testimony, how should an expert approach direct examination? How should it approach, on the other hand, cross-examination?

Fraud detection:

- What are the main characteristics of a fraud? When do frauds emerge?
- Which are the main components of anti-fraud strategies? How are they related?
- What is social engineering? What is phishing?
- What are rule-based engines? Which are their downsides?
- Why are data-driven approaches becoming more prevalent?
- Which are the main challenges to data-driven fraud detection?
- How's the fraud management cycle structured?

Machine learning for fraud detection:

- What are the differences between unsupervised learning and supervised learning?
- Compare break point analysis and peer group analysis
- What are the main approaches to hierarchical clustering? Compare them
- What are the main approaches to non-hierarchical clustering? Compare them
- What is the variable selection problem in supervised learning? Explain what characteristics of a variable may determine its use.
- How do decision tree models help to understand better other models?
- Given this starting condition and this dataset, what consideration would you make on the data? Which technique would you apply?